

#4

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of

Martin TASLER

Serial No. (unknown)

Filed herewith

METHOD AND SYSTEM FOR
IDENTIFYING A USER



CLAIM FOR FOREIGN PRIORITY UNDER 35 U.S.C. 119
AND SUBMISSION OF PRIORITY DOCUMENT

Assistant Commissioner for Patents

Washington, D.C. 20231

Sir:

Attached hereto is a certified copy of applicant's corresponding patent application filed in Germany, on 17 October 2000, under No. 10051461.8.

Applicant herewith claims the benefit of the priority filing date of the above-identified application for the above-entitled U.S. application under the provisions of 35 U.S.C. 119.

Respectfully submitted,

YOUNG & THOMPSON

By 

Robert J. Patch
Attorney for Applicant
Customer No. 000466
Registration No. 17,355
745 South 23rd Street
Arlington, VA 22202
Telephone: 703/521-2297

October 17, 2001



Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen: 100 51 461.8

Anmeldetag: 17. Oktober 2000

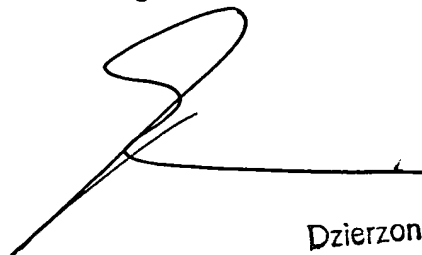
Anmelder/Inhaber: Siemens Aktiengesellschaft, München/DE

Bezeichnung: Verfahren und System zur Identifikation eines Benutzers

IPC: G 06 F 12/14

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 8. Dezember 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag



Dzierzon

CERTIFIED COPY OF
PRIORITY DOCUMENT

Beschreibung

Verfahren und System zur Identifikation eines Benutzers

5 Die Erfindung betrifft ein Verfahren zur Identifikation eines Benutzers, bei dem mindestens ein personenindividuelles Merkmal des Benutzers von einem zentralen Server abgefragt und von einem Eingabegerät einer benutzerseitigen Rechneinrichtung über eine Telekommunikationsverbindung, insbesondere
10 über das Internet an den zentralen Server übermittelt und mit gespeicherten Benutzerdaten verglichen wird.

Es sind Identifikationsverfahren für Benutzer bekannt, bei denen eine Geheimzahl oder ein Passwort z.B. über das Internet abgefragt und von dem Benutzer an einen zentralen Server
15 übermittelt werden. Diese Daten werden mit auf dem Server gespeicherten Daten verglichen. Bei Übereinstimmung kann beispielsweise ein Bezahlvorgang freigegeben werden oder das Identifikationsverfahren dient dazu, einen bestimmten geschützten Bereich im Internet für den identifizierten Benutzer frei zu geben. Die große und in den letzten Jahren ständig wachsende Zahl derartiger Systeme bringt es mit sich,
20 dass ein Benutzer eine steigende Zahl von Geheimzahlen, PIN-Nummern oder Passwörtern auswendig lernen muss. Werden diese Daten vom Benutzer aufgeschrieben, so besteht ein großes Missbrauchsrisiko, wenn diese schriftlichen Notizen verloren gehen oder gestohlen werden, da der zentrale Serverrechner nicht feststellen kann, ob es sich bei dem Benutzer um den rechtmäßigen Besitzer der Zugangsdaten handelt.
25

30

Um derartige Probleme zu vermeiden, sind weiterhin Identifikationsverfahren bekannt, bei denen ein persönliches Merkmal, insbesondere ein körperspezifisches Merkmal eines Benutzers überprüft wird. Gebräuchlich sind insbesondere Verfahren, die
35 ein Abbild der Iris des menschlichen Auges erstellen sowie Verfahren, bei denen ein Fingerabdruck als Identifizierungsmerkmal dient. In gleicher Weise ist vorgeschlagen worden,

die Handschrift als Identifizierungsmerkmal zu benutzen, indem ein Benutzer eine Unterschriftsprobe abgibt. Allen diesen Verfahren ist gemeinsam, dass das jeweilige körperspezifische Merkmal einmal von einer autorisierten Stelle erfasst und digitalisiert werden muss und anschließend in einer Datenbank abgelegt wird. Diese Datenbank enthält zumeist weitere benutzerspezifische Datensätze, bei denen es sich je nach Einsatzzweck beispielsweise um den Namen, die Anschrift oder eine Kundennummer des Benutzers handeln kann. Ein typisches Anwendungsgebiet für derartige Identifikationsverfahren ist die Zugangskontrolle bei Gebäuden. Das überprüfte körperspezifische Merkmal wird dabei jeweils vor Ort von einer Rechneinrichtung ausgewertet, die gegebenenfalls den Zutritt ermöglicht.

Der Erfindung liegt daher das Problem zu Grunde, ein fälschungssicheres Identifikationsverfahren anzugeben, das insbesondere auch bei Internet-Transaktionen verwendet werden kann.

Zur Lösung dieses Problems ist bei einem Verfahren der eingangs genannten Art erfindungsgemäß vorgesehen, dass das mindestens eine personenindividuelle Merkmal von dem zentralen Server aus einer Mehrzahl von Merkmalen nach dem Zufallsprinzip ausgewählt wird.

Durch die Kombination mehrerer Merkmale wird die Fälschungssicherheit beträchtlich erhöht, da es benutzerseitig nicht vorhersehbar ist, welches bzw. welche Merkmale von dem zentralen Server abgefragt und überprüft werden. Dabei ist es besonders vorteilhaft, dass der Benutzer weder Geheimzahlen noch Transaktionsnummern auswendig lernen oder bei sich tragen muss. Für die Identifikation werden vorzugsweise körperspezifische Merkmale benutzt, die der Benutzer zwangsläufig mit sich führt. Dementsprechend kann das erfindungsgemäße Identifikationsverfahren praktisch an jedem Ort durchgeführt werden, an dem ein geeignetes Eingabegerät zur Verfügung

steht. Selbst wenn der Benutzer vollkommen unvorbereitet ist und keine der ansonsten erforderlichen Unterlagen, wie beispielsweise eine Scheckkarte, mit sich führt, kann er eine Transaktion vornehmen.

5

Das erfindungsgemäße Verfahren zur Identifikation eines Benutzers kann für verschiedenartige Transaktionen verwendet werden. Es bieten sich in erster Linie Bestellungen und Käufe über das Internet an, bei denen die Bezahlung mittels des erfindungsgemäßen Verfahrens autorisiert werden kann. In gleicher Weise kann sich der Benutzer Zugang zu persönlichen Informationen verschaffen, er kann beispielsweise seine Kontoauszüge abrufen und sich dazu durch das erfindungsgemäße Verfahren legitimieren.

15

Um die Missbrauchsgefahr zu verkleinern, kann es vorgesehen sein, dass mehrere personenindividuelle Merkmale nach dem Zufallsprinzip ausgewählt und abgefragt werden. Es kann beispielsweise vorgesehen sein, dass die Iris eines Auges aufgenommen und überprüft wird, gleichzeitig wird ein Fingerabdruck desselben Benutzers überprüft. Erst bei Übereinstimmung beider Merkmale wird die entsprechende Aktion, beispielsweise ein Kauf, abgewickelt.

20

Besonders sicher und zuverlässig sind Identifikationsverfahren, bei denen der Abdruck wenigstens eines Fingers oder das Abbild der Iris eines Auges als Merkmale dienen. In gleicher Weise lässt sich eine Stimmprobe des Benutzers oder eine Unterschriftsprobe als Prüfmerkmal verwenden, da diese für die jeweilige Person individuell sind. Ebenso kann mit einer Kamera ein Teil des Körpers oder ein Teil des Körperprofils aufgenommen und mit zuvor gespeicherten Daten verglichen werden. In der Erprobung sind auch Verfahren, bei denen der so genannte „genetische Fingerabdruck“ als Identifizierungsmerkmal dient. Besonders bevorzugt werden dabei nichtinvasive Verfahren, die den Benutzer nicht beeinträchtigen. Diese kör-

30

35

perspezifischen Merkmale sind in einer ersten Merkmalsgruppe gespeichert.

Es ist zweckmäßig, in einer zweiten Merkmalsgruppe weitere
5 personenindividuelle Merkmale wie beispielsweise den Benutzernamen, die Anschrift, das Geburtsdatum, die Benutzer- oder Kundennummer oder eine Geheimzahl zu speichern. Der Server kann analog auch aus dieser zweiten Merkmalsgruppe wenigstens ein Merkmal auswählen und abfragen.

10 Bei dem erfindungsgemäßen Verfahren wird vorzugsweise wenigstens ein Merkmal aus der ersten Merkmalsgruppe mit körperspezifischen Merkmalen gewählt, die ein besonders hohes Maß an Sicherheit bieten.

15 In einer Weiterbildung der Erfindung ist vorgesehen, dass die Datenübertragung verschlüsselt erfolgt. In erster Linie ist es sinnvoll, die von dem Eingabegerät ermittelten Daten mit dem personenindividuellen Merkmal zu verschlüsseln, damit
20 diese von unberechtigten Dritten nicht gelesen und genutzt werden können.

Das erfindungsgemäße Identifikationsverfahren lässt sich ebenfalls für die Erstellung einer elektronischen Signatur bei
25 einer elektronischen Mitteilung verwenden, so dass der Empfänger dieser Mitteilung absolut sicher sein kann, dass die Mitteilung tatsächlich von dem angegebenen Absender stammt.

Die Erfindung betrifft ferner ein System zur Identifikation
30 eines Benutzers mit mindestens einem zentralen Server mit einer Datenbank mit personenindividuellen Merkmalen von Benutzern, mit mindestens einer externen, mit dem Server über eine Telekommunikationsverbindung, insbesondere über das Internet kommunizierenden benutzerseitigen Rechnereinrichtung mit
35 mindestens einem Eingabegerät, über welches mindestens ein personenindividuelles Merkmal des Benutzers von dem Server abfragbar und an diesen übermittelbar ist, wobei das abgefragte

personenindividuelle Merkmal von dem zentralen Server aus einer Mehrzahl von Merkmalen nach dem Zufallsprinzip auswählbar ist.

- 5 Eine Komponente des erfindungsgemäßen Identifikationssystems kann ein herkömmlicher Personal Computer sein, der als benutzerseitige Rechnereinrichtung dient. An diesen ist mindestens ein Eingabegerät angeschlossen, bei dem es sich beispielsweise um eine Digitalkamera oder ein Mikrofon handeln kann. Die
10 Eingabegeräte wandeln die Bilder bzw. Töne in digitale Daten um, die anschließend von dem Computer über das Internet an den zentralen Server übermittelt werden. Alternativ bzw. zusätzlich kann auch ein Eingabegerät zum Erfassen eines Fingerabdrucks oder ein Mittel zum Erfassen einer Unterschriftsprobe vorgesehen sein. In einer Weiterbildung der Erfindung
15 ist vorgesehen, dass die benutzerseitige Rechnereinrichtung ein Eingabegerät zum Erfassen bzw. Auswerten des genetischen Fingerabdrucks des Benutzers aufweist. Es können auch mehrere unterschiedliche Eingabegeräte an einen bestimmten benutzerseitigen Rechner angeschlossen sein. Ebenso können die Eingabegeräte mit herkömmlichen Eingabegeräten wie einem Magnetkartenleser und einer Zahlen- oder Buchstabentastatur kombiniert sein.
20
- 25 Bevorzugt werden Identifikationssysteme, die mehrere zentrale Server mit identischen Datenbanken aufweisen. Auf diese Weise wird eine besonders hohe Ausfallsicherheit gewährleistet. Wichtig ist in diesem Fall, dass die Datensätze der verschiedenen Server regelmäßig abgeglichen werden, so dass auf allen
30 Servern identische Datensätze gespeichert sind.

Zur Verhütung von Missbrauch ist es vorteilhaft, wenn das System ein Mittel zur Ver- und oder Entschlüsselung von Daten umfasst. Dieses Mittel kann als Softwareprogramm ausgebildet
35 sein, so dass die Ver- und Entschlüsselung der Daten automatisiert erfolgen kann. Diese Software kann auch Teil der

Software sein, die zur Erfassung und Digitalisierung des personenindividuellen Merkmals des Benutzers dient.

Die Erfindung wird nachfolgend unter Bezugnahme auf die Figur
5 anhand eines besonders geeigneten Ausführungsbeispiels näher erläutert.

In der Figur sind die Komponenten des erfindungsgemäßen Systems zur Identifikation eines Benutzers schematisch dargestellt. Das System 1 besteht aus dem zentralen Server 2, bei dem es sich um ein Computersystem handelt und das eine Datenbank mit einer Vielzahl von benutzerspezifischen Datensätzen 3, 4 aufweist, von denen zwei beispielhaft dargestellt sind. Der erste Datensatz 3 enthält eine erste Merkmalsgruppe 3a mit personenindividuellen Merkmalen, zu denen ein Fingerabdruck, eine Abbildung des Kopfumrisses und eine Stimmprobe des Benutzers gehören. Für denselben Benutzer sind in einer zweiten Merkmalsgruppe 3b weitere personenindividuelle Merkmale gespeichert, bei denen es sich um den Namen und die Anschrift des Benutzers sowie um Bankkontoinformationen handelt.
15
20

Der Server 2 enthält außerdem einen Datensatz 4 mit Daten eines anderen Benutzers. Die Daten des Datensatzes 4 sind ebenfalls in die Merkmalsgruppen 4a und 4b unterteilt.
25

Die Datensätze der verschiedenen Benutzer weisen jeweils die gleiche Datenstruktur auf, sie werden bei neuen Benutzern einmal erfasst und auf dem Server 2 gespeichert.
30

Zur Identifikation desjenigen Benutzers, dem der Datensatz 3 zugeordnet ist, wählt der zentrale Server 2 durch ein Softwareprogramm mindestens eines der personenindividuellen Merkmale aus der ersten Merkmalsgruppe 3a aus und übermittelt das ausgewählte Merkmal 5 über eine Internetverbindung 6 an eine benutzerseitige Rechneereinrichtung 7, die aus einem Personal Computer 8 mit einem Bildschirm 9 und einer Eingabetastatur
35

10 besteht. Der Personal Computer 8 ist in bekannter Weise,
beispielsweise über ein nicht dargestelltes Modem mit dem In-
ternet 6 verbunden. An den Personal Computer 8 sind in dem
dargestellten Ausführungsbeispiel eine Digitalkamera 11 und
5 ein Magnetkartenleser 12 angeschlossen.

Nachdem der zentrale Server 2 aus der Mehrzahl von personen-
individuellen Merkmalen der Merkmalsgruppe 3a wenigstens ein
Merkmal 5 ausgewählt hat, sendet er an die benutzerseitige
10 Rechnereinrichtung 7 eine Abfrage, durch die er das ausge-
wählte Merkmal 5 anfordert. Von dem Server 2 wird also nicht
das Merkmal selbst in digitalisierter Form versendet, sondern
die Rechnereinrichtung 7 wird aufgefordert, das Merkmal zu
senden. Der Benutzer erhält auf dem Bildschirm 9 eine Auffor-
15 derung, ein bestimmtes Merkmal nachzuweisen. Wie in der Figur
zu erkennen ist, ist die benutzerseitige Rechnereinrichtung 7
zur Aufnahme von Bilddaten mittels der Digitalkamera 11 aus-
gebildet. Der Benutzer kann somit aufgefordert werden, eine
Abbildung seiner Kopfkontur aufnehmen zu lassen, die an-
20 schließend in digitalisierter Form von der Digitalkamera 11
über die Rechnereinrichtung 7 über das Internet 6 an den
zentralen Server 2 übermittelt wird. Dieser überprüft mittels
des Softwareprogramms, ob dieses Merkmal mit dem angeforder-
ten Merkmal identisch ist. Bei Übereinstimmung erfolgt eine
25 Rückmeldung von dem zentralen Server 2 über die Internetver-
bindung 6 an die Rechnereinrichtung 7, so dass die beabsich-
tigte Transaktion, bei der es sich um einen Bezahlungsvorgang
oder eine Bestellung handeln kann, durch die Rechnereinrich-
tung 7 durchgeführt werden kann. Die Auswahl des jeweils ab-
30 gefragten Merkmals erfolgt durch einen Zufallgenerator. Neben
dem wenigstens einen personenindividuellen Merkmal kann der
Server 2 ein weiteres Merkmal aus der ersten Merkmalsgruppe
3a oder der zweiten Merkmalsgruppe 3b abfragen. Es wird je-
doch in jedem Fall wenigstens ein Merkmal aus der ersten
35 Merkmalsgruppe 3a abgefragt. Bei den Merkmalen der zweiten
Merkmalsgruppe 3b kann es sich beispielsweise um den Benut-
zernamen, aber auch um auf einer Karte, beispielsweise einer

Magnet- oder Chipkarte gespeicherte Daten handeln. Zum Auslesen dieser Daten dient der ebenfalls an die Rechneinrichtung 7 angeschlossene Magnetkartenleser 12.

- 5 Der zentrale Server 2 ist mit einer Vielzahl von externen, benutzerseitigen Rechneinrichtungen über das Internet verbunden. In der Figur ist beispielhaft noch eine zweite Rechneinrichtung 13 dargestellt, die ebenfalls aus einem Personal Computer 14 besteht. An den Personal Computer 14 ist ein
- 10 Mikrofon 15 sowie ein Eingabegerät für die Erfassung von Fingerabdrücken, eine sogenannte „Fingerabdruckmaus“ angeschlossen. Diese Fingerabdruckmaus 16 weist ein Sensorelement 17 auf, das bei aufgelegtem Finger ein Abbild des Fingerabdrucks erfasst und dieses an den Personal Computer 14 weiterleitet.
- 15 Zur Identifikation desjenigen Benutzers, dem der Datensatz 4 zugeordnet ist, übermittelt der Server 2 eine Abfrage nach mindestens einem der personenindividuellen Merkmale aus den Merkmalsgruppen 4a und 4b über die Internetverbindung 6 an
- 20 die Rechneinrichtung 13, die das Merkmal in der beschriebenen Weise erfasst, digitalisiert und an den Server 2 übermittelt. Zur Sicherheit werden sämtliche über die Internetverbindung 6 übertragenen Daten verschlüsselt.

- 25 Die einzelnen benutzerseitigen Rechneinrichtungen 7, 13 sind vollkommen unabhängig voneinander und können sehr weit entfernt voneinander aufgestellt sein. Die jeweils angeschlossenen Eingabegeräte (Digitalkamera 11, Magnetkartenleser 12, Mikrofon 15, Maus 16) können in unterschiedlichen Kombinationen vorhanden sein.

Patentansprüche

1. Verfahren zur Identifikation eines Benutzers, bei dem mindestens ein personenindividuelles Merkmal des Benutzers
5 von einem zentralen Server abgefragt und von einem Eingabegerät einer benutzerseitigen Rechneinrichtung über eine Telekommunikationsverbindung, insbesondere über das Internet an den zentralen Server übermittelt und mit gespeicherten Benutzerdaten verglichen wird, d a d u r c h g e k e n n -
10 z e i c h n e t , dass das mindestens eine personenindividuelle Merkmal von dem zentralen Server aus einer Mehrzahl von Merkmalen nach dem Zufallsprinzip ausgewählt wird.
2. Verfahren nach Anspruch 1, d a d u r c h g e -
15 k e n n z e i c h n e t , dass mehrere personenindividuelle Merkmale nach dem Zufallsprinzip ausgewählt und abgefragt werden.
3. Verfahren nach einem der vorangehenden Ansprüche,
20 d a d u r c h g e k e n n z e i c h n e t , dass aus einer ersten Merkmalsgruppe, umfassend den Abdruck wenigstens eines Fingers und/oder das Abbild der Iris wenigstens eines Auges und/oder eine Stimmprobe und/oder eine Unterschriftsprobe und/oder eine Abbildung wenigstens eines Teils des Be-
25 nutzers und/oder den genetischen Fingerabdruck wenigstens ein Merkmal ausgewählt und abgefragt wird.
4. Verfahren nach einem der vorangehenden Ansprüche,
d a d u r c h g e k e n n z e i c h n e t , dass aus
30 einer zweiten Merkmalsgruppe, umfassend den Benutzernamen und/oder die Anschrift und/oder das Geburtsdatum und/oder eine Benutzernummer und/oder eine Geheimzahl wenigstens ein Merkmal ausgewählt und abgefragt wird.
- 35 5. Verfahren nach Anspruch 3 oder 4, d a d u r c h g e k e n n z e i c h n e t , dass in jedem Fall wenigstens ein Merkmal aus der ersten Merkmalsgruppe gewählt wird.

6. Verfahren nach einem der vorangehenden Ansprüche, dadurch gekennzeichnet, dass die Datenübertragung verschlüsselt erfolgt.

5

7. System zur Identifikation eines Benutzers mit mindestens einem zentralen Server mit einer Datenbank mit personenindividuellen Merkmalen von Benutzern, mit mindestens einer externen, mit dem Server über das Internet kommunizierenden benutzerseitigen Rechneinrichtung mit mindestens einem Eingabegerät, über welches mindestens ein personenindividuelles Merkmal des Benutzers von dem Server abfragbar und an diesen übermittelbar ist, dadurch gekennzeichnet, dass das abgefragte personenindividuelle Merkmal (5) von dem zentralen Server (2) aus einer Mehrzahl von Merkmalen (3a, 3b, 4a, 4b) nach dem Zufallsprinzip auswählbar ist.

10

15

20

8. System nach Anspruch 7, dadurch gekennzeichnet, dass das Eingabegerät der benutzerseitigen Rechneinrichtung (7, 13) wenigstens eine Kamera (11) und/oder ein Mikrofon (15) und/oder ein Mittel (17) zum Erfassen eines Fingerabdrucks umfasst.

25

9. System nach Anspruch 7 oder 8, dadurch gekennzeichnet, dass mehrere zentrale Server mit identischen Datenbanken vorgesehen sind.

30

10. System nach einem der Ansprüche 7 bis 9, dadurch gekennzeichnet, dass der Server (2) und/oder die benutzerseitige Rechneinrichtung (7, 13) ein Mittel zur Ver- und/oder Entschlüsselung von Daten umfasst.

Zusammenfassung

Verfahren und System zur Identifikation eines Benutzers

- 5 Verfahren zur Identifikation eines Benutzers, bei dem mindestens ein personenindividuelles Merkmal des Benutzers von einem zentralen Server abgefragt und von einem Eingabegerät einer benutzerseitigen Rechneinrichtung über das Internet an den zentralen Server übermittelt und mit gespeicherten Benutzerdaten verglichen wird, wobei das mindestens eine personenindividuelle Merkmal von dem zentralen Server aus einer Mehrzahl von Merkmalen nach dem Zufallsprinzip ausgewählt wird.
- 10

FIG 1

